UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,324	08/03/2006	Syouzou Niwata	U 016425-2	6802

140   7590   05/28/2010

LADAS & PARRY LLP
26 WEST 61ST STREET
NEW YORK, NY 10023

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
05/28/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

nyuspatactions@ladas.com

	Application No.	Applicant(s)
Office Action Summary	10/588,324	NIWATA ET AL.
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *12 February 2010*.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-27* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This action is in response to the amendment filed on February 12, 2010. Claims
1-17 were previously pending consideration. Per the received amendment, claims 18-
27 are added.

2.   Claims 1-27 are currently pending consideration.

Response to Arguments

Applicant's arguments filed February 12, 2010 have been fully considered but
they are not persuasive for the following reasons:

The Applicant argues that the Cited Prior Art (CPA), Wood et a. (U.S. Patent
6,668,322), does not teach that an identification code is not necessary to establish a
session. However, the Examiner contends that there is no disclosure of such a
negative limitation in the specification or the original claims of the present application.
Furthermore, even if there was such a disclosure, Wood would disclose such an
embodiment. Wood discloses a single-sign on architecture so that once a user has
supplied the identification information, the gatekeeper can use the session token which
is issued *after* the requesting entity (user) has sent in authentication and identification
information to the authentication and identification components (column 14, lines 33-
58). Therefore, for subsequent interactions (sessions) the same session token can be
used and therefore the identification information is not needed.

Furthermore, the Applicant argues that the CPA does not disclose that an access

right is set by the client. This argument is not found persuasive. The CPA discloses

that the user is allowed to select from suitable authentication schemes and to provide a

login credential (column 13, lines 40-45). According to the CPA, different login

credentials and authentication schemes have different trust levels wherein the higher

the trust level the more resources a user will have access (column 15, lines 53-67).

Therefore, in this configuration, the user is setting the access right since the selection of

a less secure authentication scheme or less exhaustive login credential will result in a

lower trust level which may not be sufficient to support the requested access (column1

5, lines 55-64).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of
> making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
> set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-4, 9-13, 16-18, 21-24, and 27 are rejected under 35 U.S.C. 112, first

paragraph, as failing to comply with the enablement requirement. The claim(s) contains

subject matter which was not described in the specification in such a way as to enable

one skilled in the art to which it pertains, or with which it is most nearly connected, to

make and/or use the invention. The Examiner invites the Applicant to point out where in

the specification a disclosure is made of wherein "an identification code being not

necessary to be sent to the server computer in order to establish a session." The

Examiner cannot find support for such an assertion in the specification.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
> matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
> conditions and requirements of this title.

Claims 17-22 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter. Claims 17-22 are directed towards computer

readable mediums, which when given the broadest reasonable interpretation, include

both transitory and non-transitory media. When the specification is silent as to the

definition of the computer readable medium, the broadest reasonable interpretation of

the transitory medium includes signals per se. When an interpretation of a claim is

directed to a signal per se it must be rejected under 35 U.S.C. 101 as covering non-

statutory subject matter. Furthermore, the programs themselves are not statutory

subject matter either as they are not embodied on a tangible media.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 5-7, 9-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Wood et al. (U.S. Patent 6,668,322).

Regarding claims 1 and 17, Wood discloses:

A computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120) connected to the network (column 5, lines 46-55);

a plurality of client computers (11, 12, 21) connectable to the network; and

portable information recording media (R11, R12, R21) issued respectively to individual users for use upon connection to the client computers (column 5, lines 46-55);

wherein a unique identification code (ID(11), ID(12), ID(21)) is recorded in each of the client computers (11, 12, 21) so as to enable distinction from other client computers, an identification code (ID(11), ID(12), ID(21)) that corresponds to a specific identification code recorded in a specific client computer is recorded in each of the portable information recording media (R11, R12, R21) (column 12, lines 50-57), and

each of the client computers (11, 12, 21) comprises an interface means (11D) for connecting a portable information recording medium (R11, R12, R21), an identification code comparing means (11C) that compares an identification code recorded in a currently connected portable information recording medium (R11) and an identification code recorded in itself, an access right setting means (11B) that sets a predetermined access right based on a comparison result, and a server access means (11A) that

performs access to the server computer within a range of the access right that has been

set (column 11, lines 35-67, column 12, lines 50-65).

Regarding claims 2 and 18, Wood discloses:

A computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120) connected to the network (column 5, lines 46-55);

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); and

portable information processing devices (P11) issued respectively to individual

users for use upon connection to the client computers (column 5, lines 46-55, column

12, lines 50-57); wherein

a unique identification code (ID(11), ID(12), ID(21)) is recorded in each of the

client computers (11, 12, 21) so as to enable distinction from other client computers

(column 12, lines 50-57),

an identification code (ID(11)) that corresponds to a specific identification code

recorded in a specific client computer is recorded in each of the portable information

processing devices (P11),each of the client computers (11, 12, 21) comprises an

interface means (11D) for connecting a portable information processing device (P11),

and a server access means (11A) that performs access to the server computer (110,

120) within a range of an access right that is transmitted from a currently connected

portable information processing device (P11) (column 12, lines 50-57), and

each of the portable information processing devices (P11) comprises an

identification code comparing means (11E) that compares an identification code (ID(11))

recorded in a currently connected client computer (11) and an identification code

(ID(11)) recorded in itself, an access right setting means (11F) that sets a

predetermined access right based on a comparison result, and an access right

transmitting means (11G) that transmits, to the currently connected client computer

(11), the access right that has been set (column 11, lines 35-67, column 12, lines 50-

65).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Wood discloses:

The computer system according to claim 1, wherein

the access right setting means (11B, 11F) sets a first access right when the

comparison result indicates matching and sets a second access right, with more

restrictions than the first access right, when the comparison result indicates

mismatching (column 11, lines 36-67, column 12, lines 50-65).

Regarding claims 5 and 19, Wood discloses:

A computer system comprising: a network (100) (column 5, lines 46-55); a server

computer (110, 120) connected to the network (column 5, lines 46-55); a plurality of

client computers (11, 12, 21) connectable to the network (column 5, lines 46-55); and

portable information recording media (R11, R12, R21) issued respectively to individual

users for use upon connection to the client computers (column 5, lines 46-55); wherein

environment information (ENV(11), ENV(12), ENV(21)) that indicates a specific

network environment that is obtained when a client computer (11, 12, 21) is connected

to a specific location of the network (100) is recorded in each of the portable information

recording media (R11, R12, R21) (column 6, lines 7-22), and

each of the client computers (11, 12, 21) comprises an interface means (11D) for

connecting a portable information recording medium (R11, R12, R21), an environment

comparing means (11H) that compares a network environment indicated by

environment information (ENV(11)) recorded in a currently connected portable

information recording medium (R11) and a current network environment of itself, an

access right setting means (11B) that sets a predetermined access right based on a

comparison result, and a server access means (11A) that performs access to the server

computer within a range of the access right that has been set (column 6, lines 7-22,

column 11, lines 35-67, column 12, lines 50-65).

Regarding claims 6 and 20, Wood discloses:

A computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120) connected to the network (column 5, lines 46-55);

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); and

portable information processing devices (P11) issued respectively to individual

users for use upon connection to the client computers (column 5, lines 46-55); wherein

environment information that indicates a specific network environment that is

obtained when a client computer (11, 12, 21) is connected to a specific location of the

network (100) is recorded in each of the portable information processing devices

(P11),each of the client computers (11, 12, 21) comprises an interface means (11D) for

connecting a portable information processing device (P11), and a server access means

(11A) that performs access to the server computer (110, 120) within a range of an

access right that is transmitted from a currently connected portable information

processing device (P11) (column 6, lines 7-22), and

each of the portable information processing devices (P11) comprises an

environment comparing means (11I) that compares a network environment of a

currently connected client computer and a network environment indicated by

environment information (ENV(11)) recorded in itself, an access right setting means

(11F) that sets a predetermined access right based on a comparison result, and an

access right transmitting means (11G) that transmits, to the currently connected client

computer (11), the access right that has been set (column 6, lines 7-22, column 11,

lines 35-67, column 12, lines 50-65).

Claim 7 is rejected as applied above in rejecting claim 5. Furthermore, Wood discloses:

The computer system according to claim 5, wherein

the access right setting means (11B, 11F) sets a first access right when the

comparison result indicates matching and sets a second access right, with more

restrictions than the first access right, when the comparison result indicates

mismatching (column 11, lines 36-67, column 12, lines 50-65).

Regarding claims 9 and 21, Wood discloses:

    A computer system comprising:

    a network (100) (column 5, lines 46-55);

    a server computer (110, 120) connected to the network; a plurality of client

computers (11, 12, 21) connectable to the network (column 5, lines 46-55); and

    portable information recording media (R11, R12, R21) issued respectively to

individual users for use upon connection to the client computers; wherein

    a unique identification code (ID(11), ID(12), ID(21)) is recorded in each of the

client computers (11, 12, 21) so as to enable distinction from other client computers

(column 5, lines 46-55),

    an identification code (ID(11), ID(12), ID(21)) that corresponds to a specific

identification code recorded in a specific client computer and environment information

(ENV(11), ENV(12), ENV(21)) that indicates a specific network environment that is

obtained when a client computer (11, 12, 21) is connected to a specific location of the

network (100) are recorded in each of the portable information recording media (R11,

R12, R21) (column 6, lines 7-22), and

    each of the client computers (11, 12, 21) comprises an interface means (11D) for

connecting a portable information recording medium (R11, R12, R21), an identification

code comparing means (11C) that compares an identification code (ID(11)) recorded in

a currently connected portable information recording medium (R11) and an identification

code (ID(11)) recorded in itself, an environment comparing means (11H) that compares

a network environment indicated by environment information (ENV(11)) recorded in a

currently connected portable information recording medium (R11) and a current network

environment of itself, an access right setting means (11B) that sets a predetermined

access right based on comparison results, and a server access means (11A) that

performs access to the server computer within a range of the access right that has been

set (column 6, lines 7-22, column 11, lines 35-67, column 12, lines 50-65).

Regarding claims 10 and 22, Wood discloses:

A computer system comprising:

a network (100) (column 5, lines 46-55); a server computer (110,120) connected

to the network (column 5, lines 46-55);

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); and

portable information processing devices (P11) issued respectively to individual

users for use upon connection to the client computers (column 5, lines 46-55); wherein

a unique identification code (ID(11), ID(12), ID(21)) is recorded in each of the

client computers (11, 12, 21) so as to enable distinction from other client computers

(column 12, lines 50-57),

an identification code (ID(11), ID(12), ID(21)) that corresponds to a specific

identification code recorded in a specific client computer and environment information

(ENV(11), ENV(12), ENV(21)) that indicates a specific network environment that is

obtained when a client computer (11, 12, 21) is connected to a specific location of the

network (100) are recorded in each of the portable information processing devices

(P11),each of the client computers (11, 12, 21) comprises an interface means (11D) for

connecting a portable information processing device (P11), and a server access means

(11A) that performs access to the server computer (110, 120) within a range of an

access right that is transmitted from a currently connected portable information

processing device (P11) (column 6, lines 7-22), and

each of the portable information processing devices (P11) comprises an

identification code comparing means (11E) that compares an identification code (ID(11))

recorded in a currently connected client computer (11) and an identification code

(ID(11)) recorded in itself, an environment comparing means (11I) that compares a

network environment of the currently connected client computer and a network

environment indicated by environment information (ENV(11)) recorded in itself, an

access right setting means (11F) that sets a predetermined access right based on

comparison results, and an access right transmitting means (11G) that transmits, to the

currently connected client computer (11), the access right that has been set (column 6,

lines 7-22, column 11, lines 35-67, column 12, lines 50-65).

Claim 11 is rejected as applied above in rejecting claim 9. Furthermore, Wood

discloses:

The computer system according to claim 9, wherein

the access right setting means (11B, 11F) sets a first access right when the result of comparison by the identification code comparing means (11C, 11E) indicates matching, sets a second access right, with more restrictions than the first access right, when the result of comparison by the identification code comparing means (11C, 11E) indicates mismatching but the result of comparison by the environment comparing means (11H, 11I) indicates matching, and sets a third access right, with even more restrictions than the second access right, when neither of the comparison results indicates matching (column 11, lines 36-67, column 12, lines 50-65).

Claim 12 is rejected as applied above in rejecting claim 9. Furthermore, Wood discloses:

The computer system according to claim 9, wherein

the access right setting means (11B, 11F) sets a first access right when both the result of comparison by the identification code comparing means (11C, 11E) and the result of comparison by the environment comparing means (11H, 11I) indicate matching, sets a second access right, with more restrictions than the first access right, when the result of comparison by the identification code comparing means (11C, 11E) indicates matching but the result of comparison by the environment comparing means (11H, 11I) indicates mismatching, and sets a third access right, with even more restrictions than the second access right, when neither of the comparison results indicates matching (column 11, lines 36-67, column 12, lines 50-65).

Regarding claim 13, Wood discloses:

An access right setting method for a computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120) connected to the network (column 5, lines 46-55);

and

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55);

the method setting an access right when each individual user uses a client

computer to access the server computer and comprising:

a preparation step, wherein a portable information processing device (P11), to be

used by connecting to a client computer (11, 12, 21), is issued to each individual user,

and an identification code (ID(11)), corresponding to a unique identification code that is

recorded in a specific client computer (11) and enables distinction of the specific client

computer from other client computers, is recorded in the portable information

processing device (column 12, lines 50-57); and

an access right setting step, wherein when a user connects a predetermined

portable information processing device (P11), issued to him/herself, to a predetermined

client computer (11) and performs a login procedure on the predetermined client

computer, the predetermined client computer (11) or the predetermined portable

information processing device (P11) is made to compare an identification code (ID(11))

recorded in the predetermined client computer (11) with an identification code (ID(11))

recorded in the predetermined portable information processing device (P11) and set a

predetermined access right based on a comparison result (column 12, lines 50-57);

wherein when in the access right setting step, the comparison result indicates

mismatching, an access right with more restrictions than when the comparison result

indicates matching is set (column 11, lines 35-67, column 12, lines 50-65).

Regarding claim 14, Wood discloses:

An access right setting method for a computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120) connected to the network (column 5, lines 46-55);

and

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); the method setting an access right when each individual user uses a client

computer to access the server computer and comprising:

a preparation step, wherein a portable information processing device (P11), to be

used by connecting to a client computer (11, 12, 21), is issued to each individual user,

and environment information (ENV(11)) that indicates a specific network environment

that is obtained when a client computer (11) is connected to a specific location of the

network (100) is recorded in the portable information processing device (column 6, lines

7-22); and

an access right setting step, wherein when a user connects a predetermined

portable information processing device (P11), issued to him/herself, to a predetermined

client computer (11) and performs a login procedure on the predetermined client

computer, the predetermined client computer (11) or the predetermined portable

information processing device (P11) is made to compare a current network environment

of the predetermined client computer (11) with a network environment indicated by

environment information (ENV(11)) recorded in the predetermined portable information

processing device (P11) and set a predetermined access right based on a comparison

result (column 6, lines 7-22, column 11, lines 35-67, column 12, lines 50-65);

wherein when in the access right setting step, the comparison result indicates

mismatching, an access right with more restrictions than when the comparison result

indicates matching is set (column 11, lines 35-67, column 12, lines 50-65).

Regarding claim 15, Wood discloses:

An access right setting method for a computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120), connected to the network (column 5, lines 46-55);

and

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); the method setting an access right when each individual user uses a client

computer to access the server computer and comprising:

a preparation step, wherein a portable information processing device (P11), to be

used by connecting to a client computer (11, 12, 21), is issued to each individual user,

and an identification code (ID(11)), corresponding to a unique identification code that is

recorded in a specific client computer (11) and enables distinction of the specific client

computer from other client computers, and environment information (ENV(11)) that

indicates a specific network environment that is obtained when a client computer (11) is

connected to a specific location of the network (100) are recorded in the portable

information processing device (column 6, lines 7-22, column 12, lines 50-57); and

an access right setting step, wherein when a user connects a predetermined

portable information processing device (P11), issued to him/herself, to a predetermined

client computer (11) and performs a login procedure on the predetermined client

computer, the predetermined client computer (11) or the predetermined portable

information processing device (P11) is made to compare an identification code (ID(11))

recorded in the predetermined client computer (11) with an identification code (ID(11))

recorded in the predetermined portable information processing device (P11), compare a

current network environment of the predetermined client computer (11) with a network

environment indicated by environment information (ENV(11)) recorded in the

predetermined portable information processing device (P11), and set a predetermined

access right based on comparison results (column 6, lines 7-22, column 12, lines 50-

57);

wherein in the access right setting step, if an identification code comparison

result indicates matching, a first access right is set, if the identification code comparison

result indicates mismatching but a network environment comparison result indicates

matching, a second access right, with more restrictions than the first access right, is set,

and if neither of the comparison results indicate matching, a third access right, with

even more restrictions than the second access right, is set (column 11, lines 35-67,

column 12, lines 50-65).

Regarding claim 16, Wood discloses:

An access right setting method for a computer system comprising:

a network (100) (column 5, lines 46-55);

a server computer (110, 120), connected to the network (column 5, lines 46-55);

and

a plurality of client computers (11, 12, 21) connectable to the network (column 5,

lines 46-55); the method setting an access right when each individual user uses a client

computer to access the server computers and comprising:

a preparation step, wherein a portable information processing device (P11), to be

used by connecting to a client computer (11, 12, 21), is issued to each individual user,

and an identification code (ID(11)), corresponding to a unique identification code that is

recorded in a specific client computer (11) and enables distinction of the specific client

computer from other client computers, and environment information (ENV(11)) that

indicates a specific network environment that is obtained when a client computer (11) is

connected to a specific location of the network (100) are recorded in the portable

information processing device (column 6, lines 7-22, column 12, lines 50-57); and

an access right setting step, wherein when a user connects a predetermined

portable information processing device (P11), issued to him/herself, to a predetermined

client computer (11) and performs a login procedure on the predetermined client

computer, the predetermined client computer (11) or the predetermined portable

information processing device (P11) is made to compare an identification code (ID(11))

recorded in the predetermined client computer (11) with an identification code (ID(11))

recorded in the predetermined portable information processing device (P11), compare a

current network environment of the predetermined client computer (11) with a network

environment indicated by environment information (ENV(11)) recorded in the

predetermined portable information processing device (P11), and set a predetermined

access right based on comparison results (column 6, lines 7-22, column 12, lines 50-

57);

wherein in the access right setting step, if both an identification code comparison

result and a network environment comparison result indicate matching, a first access

right is set, if the identification code comparison result indicates matching but the

network environment comparison result indicates mismatching, a second access right,

with more restrictions than the first access right, is set, and if neither of the comparison

results indicate matching, a third access right, with even more restrictions than the

second access right, is set (column 11, lines 35-67, column 12, lines 50-65).

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Wood

discloses:

A program for making a computer function as a client computer in the computer

system according to claim 1 or a computer-readable recording medium recording the

program (column 12 lines 50-57, column 11, lines 35-67, column 12, lines 50-65).

Claim 23 is rejected as applied above in rejecting claim 2. Furthermore, Wood

discloses:

The computer system according to claim 2, wherein

the access right setting means (11B, 11F) sets a first access right when the

comparison result indicates matching and sets a second access right, with more

restrictions than the first access right, when the comparison result indicates

mismatching (column 11, lines 36-67, column 12, lines 50-65).

Claim 25 is rejected as applied above in rejecting claim 6. Furthermore, Wood

discloses:

The computer system according to claim 6, wherein

the access right setting means (11B, 11F) sets a first access right when the

comparison result indicates matching and sets a second access right, with more

restrictions than the first access right, when the comparison result indicates

mismatching (column 11, lines 36-67, column 12, lines 50-65).

Claim 27 is rejected as applied above in rejecting claim 10. Furthermore, Wood

discloses:

The computer system according to claim 10, wherein

the access right setting means (11B, 11F) sets a first access right when the

result of comparison by the identification code comparing means (11C, 11E) indicates

matching, sets a second access right, with more restrictions than the first access right,

when the result of comparison by the identification code comparing means (11C, 11E)

indicates mismatching but the result of comparison by the environment comparing

means (11H, 11I) indicates matching, and sets a third access right, with even more

restrictions than the second access right, when neither of the comparison results

indicates matching (column 11, lines 36-67, column 12, lines 50-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 8, 24 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable

over Wood et al. (U.S. Patent 6,668,322) in view of Richmond et al. (U.S. Patent

6,990,592).

Claim 4 is rejected as applied above in rejecting claim 1. Wood does not

explicitly disclose a MAC address provided to a LAN communication circuit which is

used as a unique ID for the client computer. Richmond, in an analogous art, discloses

using a MAC address or an IP address, as a device identifier in a comparison step

verifying the identity of a client (Richmond: column 27, lines 44-55). Wood uses many

factors in the credential, and could be easily extended to include other information such as the MAC or IP address (Wood: column 12, lines 50-60). Therefore, it would have been obvious to use a MAC or an IP address, as is used in Richmond, as a device identifier as disclosed in Richmond to determine the identity of the user of the user device (Richmond: column 27, lines 50-55)

Claim 8 is rejected as applied above in rejecting claim 5. Wood does not explicitly disclose an IP address being used by the client computer as environmental information. Richmond, in an analogous art, discloses using a MAC address or an IP address, as a device identifier in a comparison step verifying the identity of a client (Richmond: column 27, lines 44-55). Wood uses many factors in the environmental information, and could be easily extended to include other information such as the MAC or IP address (Wood: column 6, lines 7-22). Therefore, it would have been obvious to use a MAC or an IP address, as is used in Richmond, as a device identifier as disclosed in Richmond to determine the identity of the user of the user device (Richmond: column 27, lines 50-55).

Claim 24 is rejected as applied above in rejecting claim 5. Wood does not explicitly disclose a IP address being used by the client computer as environmental information. Richmond, in an analogous art, discloses using a MAC address or an IP address, as a device identifier in a comparison step verifying the identity of a client (Richmond: column 27, lines 44-55). Wood uses many factors in the environmental

information, and could be easily extended to include other information such as the MAC

or IP address (Wood: column 6, lines 7-22). Therefore, it would have been obvious to

use a MAC or an IP address, as is used in Richmond, as a device identifier as disclosed

in Richmond to determine the identity of the user of the user device (Richmond: column

27, lines 50-55).

Claim 26 is rejected as applied above in rejecting claim 6. Wood does not

explicitly disclose a MAC address provided to a LAN communication circuit which is

used as a unique ID for the client computer. Richmond, in an analogous art, discloses

using a MAC address or an IP address, as a device identifier in a comparison step

verifying the identity of a client (Richmond: column 27, lines 44-55). Wood uses many

factors in the credential, and could be easily extended to include other information such

as the MAC or IP address (Wood: column 12, lines 50-60). Therefore, it would have

been obvious to use a MAC or an IP address, as is used in Richmond, as a device

identifier as disclosed in Richmond to determine the identity of the user of the user

device (Richmond: column 27, lines 50-55)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is

(571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
5/22/2010
Primary Examiner, Art Unit 2431